ABSTRACT OF THE INVENTION

A drive such as a DVD-ROM drive encrypts an error code correction (ECC) block in a manner that still retains the error correction capabilities of the ECC block. Encryption is performed by generating an encryption mask including a plurality of random numbers and redundancy data. The encryption mask is bitwise XOR'ed with the ECC block. The product of the bitwise XOR is an encrypted ECC block, which can then be transmitted over an unsecured bus to a host processor. The integrity of the ECC codewords is preserved. This allows the host processor to perform some or all error correction on the encrypted ECC block. Error correction can be removed from the drive altogether, or error correction can be performed by the drive and additionally by the host processor, if necessary. User data in the ECC block can be XOR'ed entirely with random numbers, or the user data can be XOR'ed selectively with random numbers and zeros to selectively encrypt a portion of the user data. Portions of the ECC block XOR'ed with zeros or not XOR'ed at all are not encrypted. If the encrypted data is not required downstream, it is left unencrypted or it is discarded. If the encrypted data is required downstream by an entity such as a trusted decoder, information needed to decrypt the data is transmitted in a secure manner to that entity.